Akamai

WHITE PAPER

Lo stato della segmentazione nel 2023

Agevolare l'implementazione è un processo risolutivo

Sommario

Introduzione

I reparti della sicurezza IT non hanno mai avuto vita facile. Ma ora, criminali sempre più sofisticati combinano le tecniche per creare minacce più grandi e più frequenti, mettendo i team di sicurezza sotto pressione come mai prima d'ora. Nessuna azienda può operare senza una presenza online, e una violazione riuscita può causare danni ingenti, se non irreparabili, alla reputazione e al fatturato.

Come dimostrano i risultati di questo rapporto, gli attacchi stanno avendo un impatto perfino maggiore, aumentando la pressione sui responsabili della sicurezza affinché scelgano le soluzioni giuste e mantengano l'intero ambiente sicuro, senza sacrificare le performance complessive o l'innovazione.

Nell'aggiornare i risultati di questo rapporto dal 2021, abbiamo cercato di capire se la segmentazione fosse la soluzione preferita e se fosse efficace. I 1.200 intervistati hanno concordato in modo schiacciante sull'efficacia della segmentazione nel mantenere le risorse protette, ma i loro progressi complessivi nell'implementazione intorno alle applicazioni e alle risorse aziendali critiche sono stati inferiori alle aspettative. In tutte le aree geografiche, l'ostacolo numero uno è stato la mancanza di competenze nell'implementazione della segmentazione, il che suggerisce che i team potrebbero esitare a imbarcarsi in un progetto che potrebbe interrompere le performance, soprattutto data la crescente complessità degli ambienti IT.

La buona notizia? La perseveranza dà i suoi frutti. La segmentazione ha dimostrato di avere un effetto trasformativo sulla difesa per coloro che hanno segmentato la maggior parte delle risorse critiche, consentendo loro di mitigare e contenere i ransomware 11 ore più velocemente rispetto a coloro che avevano segmentato solo una risorsa. Immaginate la differenza che fanno quelle 11 ore per il vostro team, i vostri clienti, la reputazione del vostro brand e il vostro fatturato.

Gli attacchi ransomware continuano ad aumentare, così come il loro impatto

Il numero di attacchi ransomware (riusciti o meno) è raddoppiato negli ultimi due anni, passando da una media di 43 nel 2021 a 86 nel 2023. Un aumento ancora maggiore è stato riscontrato tra il primo trimestre del 2022 e il primo trimestre del 2023 tramite i dati raccolti dai siti dannosi di circa 90 diversi gruppi di ransomware. Pubblicato ad agosto 2023, il rapporto Ransomware in azione: l'evoluzione delle tecniche di sfruttamento delle vulnerabilità e l'obiettivo degli attacchi zero-day racconta di come l'uso di vulnerabilità zero-day e one-day abbia portato a un aumento del 143% delle vittime totali di ransomware a livello globale.

Non sorprende che siano ancora le aziende statunitensi ad affrontare il maggior numero di minacce ransomware (Figura 1): i team di sicurezza IT e i responsabili decisionali di questo Paese hanno registrato una media di 115 attacchi ransomware negli ultimi 12 mesi, la più alta di tutti i Paesi presi in esame.

Numero medio di attacchi ransomware negli ultimi 12 mesi per Paese

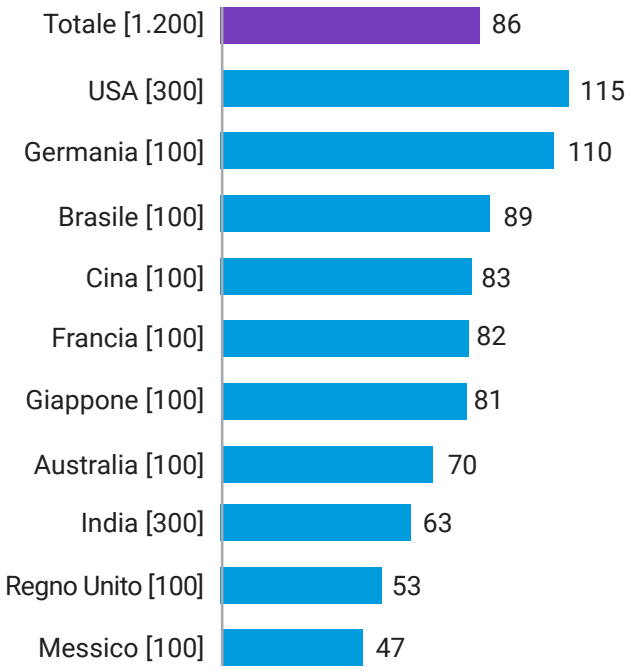

Figura 1. Quanti attacchi ransomware hanno colpito la vostra organizzazione negli ultimi 12 mesi (indipendentemente dal fatto che siano andati a buon fine o meno)? [1.200], che mostra solo il numero medio di attacchi negli ultimi 12 mesi, suddivisi per Paese.

Considerando che gli Stati Uniti sono tra i due Paesi ad aver implementato con meno probabilità la segmentazione in più di due aree aziendali di importanza critica (Figura 2), il loro primato negli attacchi ransomware e il loro basso livello di diffusione della segmentazione potrebbero essere correlati.

Naturalmente, l'elevato numero di attacchi ransomware negli Stati Uniti è probabilmente attribuibile a una serie di fattori, tra cui la notorietà di violazioni importanti come quella commessa da un gruppo di criminali informatici russi contro le agenzie federali nel 2023 e la proliferazione di dispositivi IoT negli Stati Uniti (2 miliardi in più rispetto alla Cina, seconda classificata). Il R4IoT (Ransomware-for-IoT) sfrutta i dispositivi IoT vulnerabili, come le telecamere IP, per ottenere un punto d'appoggio iniziale e poi si sposta lateralmente in una rete IT, sfruttando le pratiche di sicurezza inadeguate per tenere in ostaggio i processi mission-critical.

Gli attacchi ransomware non solo sono più frequenti a livello globale nel 2023 rispetto al 2021, ma hanno anche un impatto maggiore (Figura 3): i nostri intervistati indicano un aumento dei tempi di inattività della rete, della perdita di dati e dei danni alla reputazione, tutti fattori che alzano notevolmente la posta in gioco per i team di sicurezza. Vediamo l'effetto di questa pressione anche in termini di strategia: il numero di organizzazioni che aggiornano continuamente le strategie o le politiche di sicurezza informatica è passato dal 5% nel 2021 al 13% nel 2023, in risposta non solo ai ransomware ma anche a una superficie di attacco in costante evoluzione. La distribuzione della forza lavoro e la migrazione di applicazioni e dati nel cloud sono solo due dei fattori che influenzano quotidianamente la strategia di sicurezza.

Coloro che hanno segmentato più di due risorse/aree per Paese

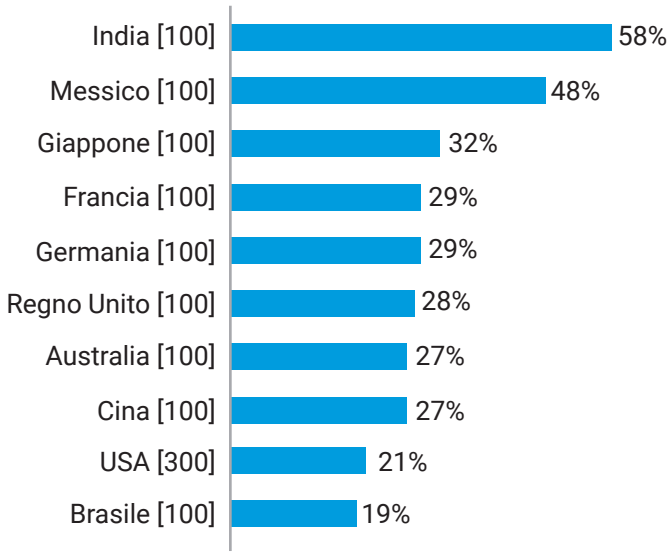

Figura 2. Per ognuna delle seguenti misure di sicurezza IT, quali sono le risorse eventualmente coperte? [1.200], che mostra le risposte per la sola misura di sicurezza della segmentazione e le percentuali che utilizzano la segmentazione per proteggere le risorse chiave, suddivise per Paese.

Impatto dei ransomware/attacchi informatici

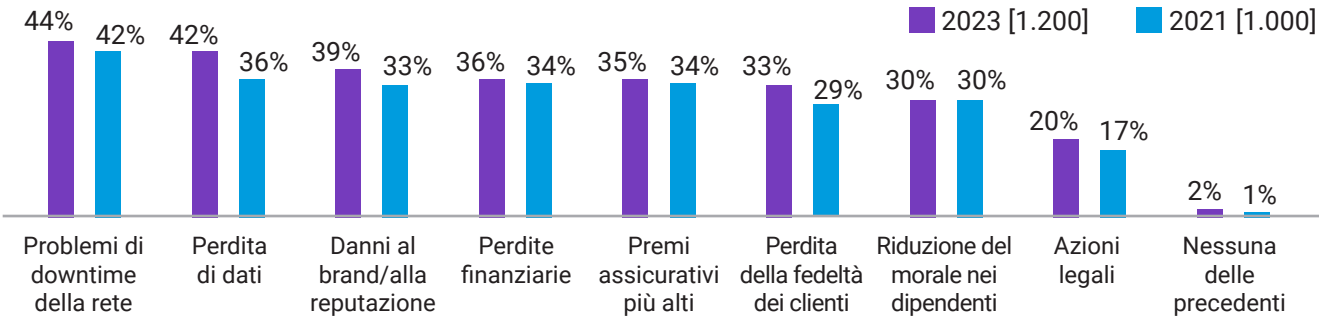

Figura 3. Quando è stato rilevato in precedenza un ransomware o un altro attacco informatico, quali dei seguenti impatti ha avuto sulla vostra organizzazione? [Dimensioni di base nel grafico], senza mostrare tutte le opzioni di risposta, suddivise per dati storici.

Risultati regionali

È più probabile che gli attacchi informatici prendano di mira le Americhe: il numero totale di attacchi ransomware è più alto nelle Americhe, con una media di 96 attacchi negli ultimi 12 mesi, rispetto agli 83 nell'area EMEA e ai 75 nell'APAC.

La segmentazione e la microsegmentazione sono considerate più importanti in APAC e nelle Americhe che in EMEA: i team di sicurezza IT e i responsabili decisionali in APAC (62%) e nelle Americhe (60%) sono più propensi ad affermare che la segmentazione della rete è estremamente importante per garantire la sicurezza della loro organizzazione rispetto a quelli in EMEA (53%).

Gli intervistati americani sono più propensi ad affermare che la microsegmentazione è la priorità assoluta (41%) rispetto alle controparti dell'APAC (35%) o dell'EMEA (23%).

Gli intervistati dell'area EMEA hanno maggiori probabilità di non aver effettuato alcuna segmentazione: è molto più probabile che le organizzazioni dichiarino di non aver segmentato alcuna risorsa critica per l'azienda in EMEA (10%) rispetto all'APAC (4%) o alle Americhe (1%).

I tassi di implementazione più lenti, cioè quelli che non hanno segmentato alcuna area, sono stati registrati nel Regno Unito (23%), dove le apparecchiature legacy vengono indicate come il principale ostacolo (46%).

Le organizzazioni dell'APAC sono quelle che hanno segmentato di più: le organizzazioni dell'APAC hanno più probabilità di aver segmentato più di due risorse critiche per l'azienda (36%) rispetto a quelle dell'EMEA (29%) o delle Americhe (26%).

Le organizzazioni, in tutte le regioni, devono affrontare delle sfide: il 97% di quelle americane afferma di aver incontrato dei problemi durante la segmentazione della rete. Una percentuale analoga è stata espressa in EMEA (94%) e APAC (97%).

Sia in EMEA che in APAC la mancanza di competenze/esperienze (38% e 43%) è il principale ostacolo alla segmentazione. Per quelli delle Americhe, l'ostacolo maggiore è rappresentato dall'aumento dei colli di bottiglia delle performance (41%).

Un numero maggiore di organizzazioni nelle Americhe considera i propri sistemi di sicurezza Zero Trust maturi: gli intervistati americani sono più propensi a dichiarare che la loro implementazione Zero Trust è pienamente completa e definita (49%) rispetto a quelli dell'APAC (35%) o dell'EMEA (33%).

La segmentazione è ampiamente riconosciuta come parte importante della strategia Zero Trust

I nostri intervistati concordano sull'importanza della segmentazione nel garantire la sicurezza della loro organizzazione, in particolare nell'affrontare le minacce informatiche. In tutti i settori, il 93% ritiene che sia fondamentale per contrastare gli attacchi dannosi, percentuale che sale al 99% per i settori manifatturiero e produttivo. Ciò potrebbe essere dovuto al fatto che questi settori dipendono fortemente da una serie di terze parti nella loro supply chain, per cui un'interruzione può avere effetti a cascata massicci sull'azienda.

Inoltre, la segmentazione contribuisce in modo determinante a un sistema Zero-Trust. Quando si cita il motivo per cui la propria organizzazione ha avviato un progetto di segmentazione, la terza risposta più comune è stata quella di far progredire la strategia Zero Trust: quasi tutti coloro che hanno effettuato una segmentazione stanno implementando o hanno già implementato un sistema di sicurezza Zero Trust (99%), anche se solo due su cinque (40%) dichiarano che il loro sistema Zero Trust è pienamente definito e completo.

A livello globale, la maggioranza degli intervistati aspira a spingersi oltre e a implementare la microsegmentazione, che protegge i carichi di lavoro delle applicazioni a livello granulare: l'89% dichiara che la microsegmentazione è almeno una priorità elevata, mentre il 34% la indica come priorità assoluta. Inoltre, il 97% dei team IT e dei responsabili delle decisioni riferisce che è stata adottata da almeno una minoranza del proprio settore. Questa percentuale scende all'80% per il settore pubblico (esclusa la sanità), una differenza attribuibile ai budget più limitati e alle infrastrutture preesistenti che pongono maggiori ostacoli all'implementazione della protezione a livello di carichi di lavoro della microsegmentazione.

La microsegmentazione

dei team di sicurezza IT e dei responsabili delle decisioni riferiscono che la microsegmentazione è stata adottata da almeno una minoranza del loro settore

Tuttavia, il settore pubblico può trarre grandi vantaggi dall'implementazione di tecniche di sicurezza avanzate come la microsegmentazione. Poiché i sistemi in questo settore non sono necessariamente progettati per interagire tra loro, mancano di interoperabilità, il che aumenta sia la probabilità di errore umano sia la probabilità di successo di un attacco informatico.

A livello di segmentazione, il 15% degli intervistati del settore pubblico dichiara di non aver messo in atto alcuna segmentazione, anche se il 93% riconosce la sua importanza. Ciò rappresenta il livello di diffusione più basso per settore, con l'ostacolo maggiore rappresentato dai requisiti di conformità (52%).

La segmentazione va bene. La microsegmentazione è ancora meglio.

La segmentazione è un approccio architetturale che divide una rete in segmenti più piccoli per migliorare le performance e la sicurezza.

La microsegmentazione divide una rete in segmenti a livello di singolo carico di lavoro, in modo da poter definire i controlli di sicurezza e la delivery di servizi per ogni singolo segmento.

Le implementazioni sono lente, ma perseverare produce risultati trasformativi

La dura realtà è che, nonostante in larga parte tutti concordino sul fatto che la segmentazione sia la chiave per fermare gli attacchi, l'implementazione della segmentazione è stata lenta, forse più di quanto ci si aspettasse. Solo il 30% delle organizzazioni ha segmentato più di due delle aree aziendali più importanti nel 2023 (rispetto al 25% nel 2021), mentre il 44% ha avviato un progetto di segmentazione della propria rete almeno due anni fa, il che suggerisce uno stallo.

La lentezza delle implementazioni è spiegata più chiaramente dai principali ostacoli incontrati dagli intervistati: mancanza di competenze/esperienze per la segmentazione (39%), aumento dei colli di bottiglia delle performance (39%) e requisiti di conformità (38%; Figura 4). Quasi tutte le aziende intervistate, indipendentemente dal settore, dall'industria o dal paese in cui operano, hanno sostenuto di incontrare gli stessi ostacoli con modalità leggermente diverse. Vale la pena notare che, sebbene la mancanza di competenze/esperienze sia la prima causa del ritardo nei progetti di segmentazione, la carenza di talenti è presente in tutta la sicurezza informatica e, con i cambiamenti che avvengono così rapidamente in questo settore, è normale rilevare carenze di competenze.

Nonostante i lenti progressi, i tassi di segmentazione stanno gradualmente aumentando. La percentuale di organizzazioni con applicazioni/dati business-critical segmentati è aumentata del 12% e quella dei server segmentati dell'8% dal 2021 al 2023.

Ostacoli incontrati durante la segmentazione della rete

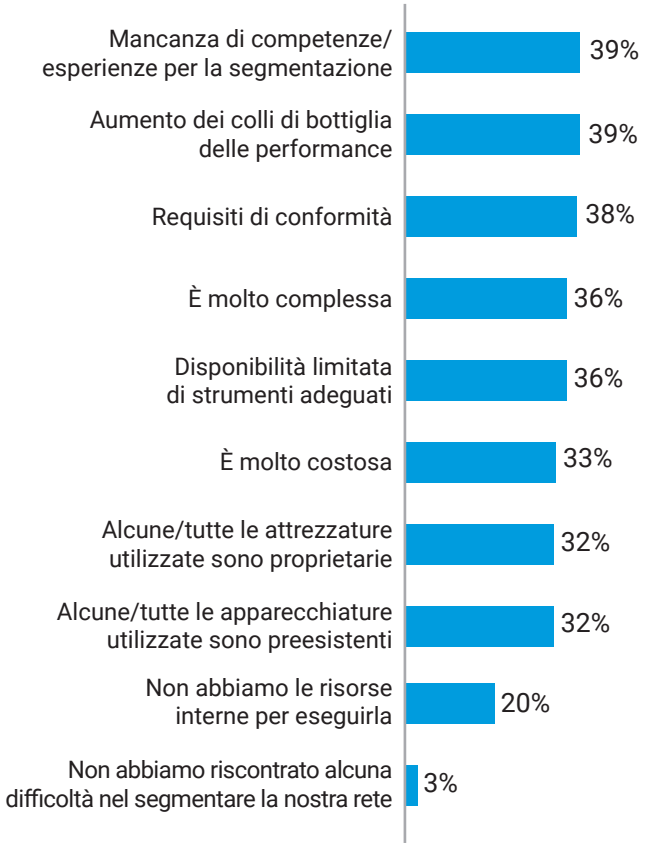

Figura 4. Quali eventuali problemi la vostra organizzazione ha incontrato/prevede di incontrare durante la segmentazione della rete? [1.187], mostrato solo a coloro che a un certo punto hanno segmentato la rete, senza mostrare tutte le opzioni di risposta.

Il risultato: la segmentazione di sei aree aziendali critiche riduce enormemente il rischio

La protezione e la segmentazione di un maggior numero di risorse rende immediatamente più sicure le organizzazioni. I team di sicurezza sono maggiormente in grado di identificare gli attacchi e possono rispondere in modo molto più efficace. L'implementazione di strategie di segmentazione immature o non ben definite non fa altro che aumentare il rischio di un'organizzazione ma, se la segmentazione viene eseguita bene, vale sicuramente tutti gli sforzi necessari per superare gli ostacoli alla sua implementazione.

I nostri risultati mostrano che, dopo una violazione, il recupero avviene 11 ore più velocemente con la segmentazione. Facciamo due calcoli: per coloro che hanno implementato la segmentazione in sei aree mission-critical, sono necessarie in media quattro ore per bloccare completamente un attacco ransomware; per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie 15 ore.

Allo stesso modo, la segmentazione consente di risparmiare 11 ore quando si limita il movimento laterale. Per coloro che hanno implementato la segmentazione in tutte e sei le aree mission-critical, sono necessarie in media tre ore per limitare in modo significativo gli spostamenti laterali di un attacco ransomware. Per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie in media 14 ore.

Considerate la differenza che fanno 11 ore per il vostro team e per contenere i costi e i danni al marchio in entrambi gli scenari.

Per contrastare un attacco

4 ore

Il tempo necessario, in media, per bloccare completamente un attacco ransomware, per coloro che hanno segmentato tutte e sei le risorse aziendali

Per coloro che hanno segmentato una sola risorsa: **15 ore**

Per limitare il movimento

3 ore

Il tempo necessario, in media, per limitare in modo significativo il movimento laterale di un attacco ransomware, per chi ha segmentato tutte e sei le risorse aziendali

Per coloro che hanno segmentato una sola risorsa: **14 ore**

In che modo una soluzione di microsegmentazione basata su software aiuta a risolvere le sfide

La microsegmentazione non solo consente un tipo di segmentazione più avanzato e granulare, ma ne semplifica anche l'implementazione.

Le soluzioni basate su software, come Akamai Guardicore Segmentation, possono essere implementate rapidamente, senza dover apportare modifiche fisiche alla rete. Non è necessario eseguire il re-IP dei nuovi segmenti o preoccuparsi della posizione fisica dei server e dei dispositivi. Ciò rende la soluzione molto più rapida e semplice da implementare rispetto agli approcci basati sull'infrastruttura, come i firewall e le VLAN. Inoltre, poiché la soluzione utilizza un driver proprietario per l'applicazione delle policy, funziona in modo eccellente su tutti i computer e i sistemi operativi: dai server bare-metal alle implementazioni multicloud, dalle tecnologie legacy come Windows Server 2003 ai più recenti dispositivi IoT/OT e alla tecnologia containerizzata. Ciò significa che dovete gestire un'unica soluzione con un'unica interfaccia per visualizzare e controllare le connessioni effettuate da diversi sistemi operativi e dispositivi nell'intero ambiente, indipendentemente dalla loro posizione fisica.

Come facilita la distribuzione

La microsegmentazione genera innanzitutto una visualizzazione interattiva di tutte le connessioni che vengono effettuate nell'ambiente, un elemento fondamentale per superare i principali ostacoli all'implementazione. Inoltre, noi di Akamai abbiamo integrato nella nostra soluzione dei modi attivi per affrontare i colli di bottiglia delle performance e i requisiti di conformità.

I colli di bottiglia delle performance non derivano necessariamente da uno sforzo tecnico del sistema causato da una soluzione di segmentazione, ma da colli di bottiglia della forza lavoro causati dalla necessità di segmentare manualmente le aree aziendali e di risolvere manualmente i problemi di tali aree quando si verificano dei problemi. Akamai si adopera per risolvere questo problema (e l'ostacolo numero uno all'implementazione, ossia la mancanza di competenze) riducendo la necessità di eseguire la segmentazione manualmente e offrendo un supporto tecnico e servizi professionali di alto livello. I nostri esperti di segmentazione collaborano con voi durante l'intero processo di implementazione per garantire il raggiungimento degli obiettivi di segmentazione nel vostro ambiente IT esclusivo.

Il supporto all'implementazione deriva anche dalla soluzione stessa: le raccomandazioni di policy basate sull'intelligenza artificiale e i modelli di policy già pronti per i casi d'uso più comuni fanno risparmiare tempo e clic, semplificano il flusso di lavoro, riducono il tempo complessivo di implementazione delle policy e prevengono le configurazioni errate dovute a errori umani. Per uno dei nostri clienti, siamo stati in grado di realizzare un progetto di segmentazione granulare che avrebbe richiesto due anni e oltre un milione di dollari di costi totali in sole sei settimane con un solo tecnico, riducendo il costo complessivo del progetto dell'85%, dimostrando che la segmentazione granulare può essere implementata in modo rapido e semplice, senza subire colli di bottiglia.

Come facilita la conformità

Molti dei nostri clienti utilizzano la nostra soluzione per garantire e attestare la conformità a una serie di mandati di conformità nazionali e internazionali, come PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR e molti altri. Questi mandati di conformità di solito richiedono che i dati in questione siano separati dagli altri sistemi dell'ambiente. Sebbene ciò possa essere proibitivo utilizzando firewall e VLAN, la nostra soluzione basata su software consente di creare segmenti specifici per i dati in questione e di applicare regole di comunicazione su chi può o non può accedere a tali dati. Utilizzando la nostra mappa visiva con visualizzazioni quasi in tempo reale e storiche, potete attestare la vostra conformità a questi mandati dimostrando fisicamente che i dati in questione non sono accessibili a utenti e computer non autorizzati.

Perseverare con la soluzione e il supporto giusti per trasformare la strategia di sicurezza

La segmentazione può essere eccessivamente difficile da implementare. Tuttavia, come dimostra questo rapporto, chi riesce a implementarla in modo efficace vede ridursi in modo massiccio il proprio rischio informatico. Una segmentazione adeguata limita il movimento laterale delle minacce e consente di reagire più rapidamente durante una violazione attiva. E dopo una violazione, le operazioni di ripristino sono più sicure e richiedono meno tempo.

Scegliere una soluzione progettata per superare le sfide comuni all'implementazione della segmentazione, e collaborare con esperti del settore durante il percorso, vi mette nella migliore posizione possibile per trasformare la vostra strategia di sicurezza. Inoltre, più aree aziendali segmentate, più fate progredire la vostra architettura Zero Trust, riducendo il rischio attuale e garantendo una difesa di prima linea contro i vettori di minaccia futuri.

Il nostro gruppo di sondaggio

Abbiamo intervistato 1.200 responsabili IT e addetti responsabili decisionali in 10 Paesi allo scopo di misurare i progressi compiuti dalle organizzazioni in termini di protezione dei loro ambienti, focalizzandoci sul ruolo della segmentazione.

Agli intervistati sono state poste domande sui loro sistemi di sicurezza IT e sulle strategie di segmentazione adottate, nonché sulle minacce che le loro organizzazioni si sono trovate ad affrontare nel 2023. Dai risultati, possiamo comprendere come le strategie di sicurezza siano cambiate a partire dal 2021 e quali aree ancora necessitino di miglioramenti.

Sono stati intervistati addetti alla sicurezza e responsabili decisionali che operano negli Stati Uniti, in Messico, in Brasile, nel Regno Unito, in Francia, Germania, Cina, India, Giappone e Australia. Tutte le aziende intervistate impiegano oltre 1.000 dipendenti e operano in vari settori e industrie.

Nota: questo campione è leggermente diverso da quello del 2021. Dimensioni del campione nel 2023: 1.200 risposte, nel 2021: 1.000 risposte. Nel 2023 sono stati intervistati anche responsabili provenienti da Australia, Giappone e Cina. I settori sono leggermente diversi rispetto al 2021. Nel 2023, ci siamo concentrati specificamente sul commercio digitale come settore a sé stante.

Per ulteriori informazioni su Akamai Guardicore Segmentation

Akamai protegge l'experience dei vostri clienti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, proteggere app e API o proteggere la vostra infrastruttura), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 10/23.

VansonBourne

Vanson Bourne è un'azienda indipendente specializzata in ricerche di mercato per il settore tecnologico. La sua reputazione di azienda in grado di offrire analisi solide e credibili si basa su principi di ricerca rigorosi e sulla capacità di raccogliere le opinioni di responsabili decisionali senior in tutti i ruoli tecnici e commerciali, in tutti i settori e in tutti i principali mercati. Per altre informazioni, visitate www.vansonbourne.com.